REMARKS

Claims 30, 32-38, 40-45, and 47-50 remain in the application. Claims 31, 39, and 46 have been cancelled, without prejudice or disclaimer, and claims 30, 32-33, 38, 40-41, 44, and 47-48 have been amended hereby.

The claims have been carefully reviewed and amended with particular attention to the points raised in the Office Action. It is submitted that no new matter has been added and no new issues have been raised by the present response.

Reconsideration is respectfully requested of the rejection of claims 30-50 under 35 U.S.C. § 102(e), as allegedly being anticipated by U.S. Patent No. 6,226,744 to Murphy et al.

Applicant has carefully considered the comments of the Office Action and the cited reference, and respectfully submits that claims 30, 32-38, 40-45, and 47-50 are patentably distinct over the cited reference for at least the following reasons.

The present invention relates to a system for allowing a user to complete a secure transaction over a network. The system includes at least a data card, a data card reader, a data processor, and an application program. The data card contains information specific to the user, including authentication and personal information. The data card reader is adapted to access at least part of the information on the data card. The data processor is in communication with the data card reader and may be connected to the network. The application program is resident on the data processor, and is configured to automatically prompt the user to enter the authentication information for comparison with the authentication information on the data card to allow the user to complete the secure transaction over the network using the user-specific information. Upon an initial use of the data card, the user is prompted to initiate the data card by inputting the authentication information and the personal information into the data processor for storage on the data card.

Murphy et al., as understood by Applicant, relates to a method and apparatus for authenticating users on a network using a smart card. The network includes a client computer and a server computer, and the client computer contains a smart card and a smart card reader. The client computer sends a request to the server to access restricted information stored within the server. The server sends a smart card interface module to the client computer, and requests an access code from a user to access the smart card. When the server receives the access code, the server accesses user information stored on the smart card utilizing the module and the access code. The server compares the user information with authentication information available only to the server. If the user information matches the authentication information, the server grants the client computer access to the restricted information.

The Office Action states that Murphy et al. discloses a system including a client computer, plural servers, a database, a smart card reader, and a smart card that stores user information (see Office Action, p. 2, ln. 23 to p. 3, ln. 10).

As understood by Applicant, the process of Murphy et al. begins with the distribution of the smart card to the user (see Murphy et al., col. 5, lns. 52-65; Fig. 3). The user inserts the card into a 3.5 inch floppy disk drive, via a "Smarty" reader, to allow access to the smart card (see id., col. 5, ln. 66 to col. 6, ln. 7; Fig. 1).

Using a web browser, the client computer of Murphy et al. accesses a gateway server via the World Wide Web (WWW) (see id., col. 6, lns. 8-63). The gateway server initiates the authentication of the user using an authentication module that determines whether the smart card is present in the client computer (see id.). When the smart card is present, the authentication module initiates a download of a smart card interface module to the client computer (see id.).

After the card interface module of Murphy et al. has been downloaded to the client computer, the card interface module is executed by the client computer (see id.). The card interface module first modifies parameters for the operating system of the client computer, and then requests a personal identification number (PIN) to access the smart card (see id.).

The authentication module then retrieves authentication information from the database, and compares the user information from the smart card with the retrieved authentication information (see id.). When the comparison indicates a match between the authentication information and the user information, the authentication module grants the user access to the restricted information (see id.).

As understood by Applicant, the smart card of Murphy et al. is configured and distributed to the user by a "certified authority" (CA) (see Murphy et al., col. 5, lns. 52-65). The user information stored on the smart card is provided by the CA (see id.). Additionally, the authentication information is stored in the database under control of the CA (see id., col. 6, lns. 32-41).

In contrast, in the system of the present invention, the user is prompted to initiate the data card upon an initial use of the data card, by inputting the authentication information and the personal information into the data processor for storage on the data card (see specification of the present application, p. 8, lns. 10-23).

Furthermore, as stated above, the authentication module of Murphy et al. initiates a download of a smart card interface module to the client computer when the authentication determines that the smart card is present. That is, as understood by Applicant, the interface module is not located on the client computer, but is instead downloaded from a remote database.

In contrast, in the presently claimed invention, an application program is resident on the data processor and is configured to automatically prompt the user to enter the authentication information for comparison with the authentication stored on the data card in order to authorize the user (see specification of the present application, p. 13, lns. 19-21).

Additionally, as understood by Applicant, the authentication method and apparatus of Murphy et al. is directed to restricting or allowing access to information stored on the server (see Murphy et al., col. 3, lns. 31-45; col. 6, lns. 43-49).

The computer system of the presently claimed invention, however, allows a user to complete a secure transaction over the network using the information specific to the user when authorized following a match of the authentication information by the application program (see specification of the present application, p. 17, lns. 12-16).

It is respectfully submitted that Murphy et al. does not disclose or suggest a computer system for allowing a user to complete a secure transaction over a network, comprising a data card which contains information specific to the user, including authentication information and personal information; a data card reader, a data processor, and an application program resident on the data processor and configured to automatically prompt the user to enter the authentication information for comparison with the authentication information stored on the data card, in order to authorize the user following a match thereof to complete the secure transaction over the network using the information specific to the user, wherein upon an initial use of the data card the user is prompted to initiate the data card by inputting the authentication information and the personal information into the data processor for storage on the data card, as described above and as recited in independent claim 30.

Accordingly, for at least the above-stated reasons, it is respectfully submitted that amended independent claim 30, and the claims depending therefrom, are patentable over the cited reference. Amended independent claims 38 and 44, and the claims depending therefrom, are believed to be patentable over the cited reference for at least similar reasons.

The references cited as of interest have been reviewed, but are not seen to show or suggest the present invention as recited in the claims.

Should the Examiner disagree, it is respectfully requested that the Examiner specify where in the cited document there is a basis for such disagreement.

The Office is hereby authorized to charge any fees which may be required in connection with this Amendment and to credit any overpayment to Deposit Account No. 03-3125.

Favorable reconsideration is earnestly solicited.

Dated: December 11, 2003

Norman H. Zivin
Reg. No. 25,385
c/o Cooper & Dunham LLP
1185 Avenue of the Americas
New York, NY 10036
(212) 278-0400
Attorney for Applicant

I hereby certify that this paper is being deposited this date with the U.S. Postal Service as first class mail addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

12/11/03

Norman H. Zivin Date
Reg. No. 25,385